JOURNAL OF NUMBER THEORY 28, 288–298 (1988)

On Power Bases in Cyclotomic Number Fields

ANDREW BREMNER

Department of Mathematics, Arizona State University, Tempe, Arizona 85287

Communicated by Hans Zassenhaus

Received February 23, 1987

The current paper considers the question of power bases in the cyclotomic number field $\mathbf{Q}(\zeta)$, $\zeta^p = 1$, p an odd prime. The ring of integers is $\mathbf{Z}[\zeta]$, and there do exist further "non-obvious" generators for this order; specifically we shall see that $\mathbf{Z}[\alpha] = \mathbf{Z}[\zeta]$ for $\alpha = \zeta + \zeta^2 + \cdots + \zeta^{(p-1)/2}$. We conjecture that, up to conjugacy, there can be no further such integral generators, and prove that this is indeed the case in $\mathbf{Q}(\zeta_7)$. © 1988 Academic Press, Inc.

1

Given an algebraic integer θ, then $\mathbf{Z}[\theta]$ is an obvious order of the number field $\mathbf{Q}(\theta)$. The question arises as to which integers α may also generate the same order, i.e., $\mathbf{Z}[\alpha] = \mathbf{Z}[\theta]$. Certainly $\mathbf{Z}[\alpha] = \mathbf{Z}[m \pm \alpha]$ for any $m \in \mathbf{Z}$; defining α, α' to be equivalent if there exists $m \in \mathbf{Z}$ with $\alpha = m \pm \alpha'$, then it suffices to consider only those α up to equivalence with $\mathbf{Z}[\alpha] = \mathbf{Z}[\theta]$. By the work of Györy [4], the set $S(\alpha)$ of such α is a finite set, and is effectively computable. The relevant bounds, based on the work of Stark, are rather large and impractical for use in specific instances, and it seems in general that $S(\alpha)$ is quite small. For example, if θ is a quadratic algebraic integer, then $S(\theta) = \{\theta\}$; and if θ is a cubic algebraic integer, it can be shown without undue difficulty that for almost all such θ, then $S(\theta)$ has at most 12 elements. (This latter proof reduces to finding binomial units in the cubic number field, to which recent results of Evertse [3] are applicable.) For an example of a power base determination in a quartic field, see Nagell [5] or Bremner [1], where a considerable amount of arithmetic is required.

0022-314X/88 $3.00

2

Let p be an odd prime and denote by ζ a primitive pth root of unity. Suppose $\alpha \in \mathbf{Z}[\zeta]$ with $\mathbf{Z}[\alpha] = \mathbf{Z}[\zeta]$; then α is of index 1 in $\mathbf{Z}[\zeta]$. The index $I(\alpha)$ of α in $\mathbf{Z}[\zeta]$ is given by the formula

$$\Delta(1, \alpha, ..., \alpha^{p-2}) = I(\alpha)\, \Delta(1, \zeta, ..., \zeta^{p-2}), \tag{1}$$

where $\Delta^2(\omega_1, ..., \omega_n)$ is the discriminant of the set of elements $\{\omega_1, ..., \omega_n\}$. Further

$$\Delta^2(1, \theta, ..., \theta^{n-1}) = (-1)^{(n(n-1))/2} \operatorname{Norm}_{\mathbf{Q}(\theta)/\mathbf{Q}}(f'(\theta)), \tag{2}$$

where f is the minimum polynomial over $\mathbf{Q}$ of θ.

Thus, the condition that $I(\alpha)$ equals 1 implies from (1), (2):

$$\operatorname{Norm}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(F'(\alpha)) = \operatorname{Norm}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(G'(\zeta)), \tag{3}$$

where $F(x)$ is the minimum polynomial over $\mathbf{Q}$ of α, and

$$G(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \tag{4}$$

is the minimum polynomial over $\mathbf{Q}$ of ζ.

Writing $F(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_{p-1})$ where $\{\alpha_i\}$ are the conjugates of α, then

$$F'(\alpha) = (\alpha-\alpha_2)\cdots(\alpha-\alpha_{p-1}). \tag{5}$$

Similarly

$$G'(\zeta) = (\zeta-\zeta^2)\cdots(\zeta-\zeta^{p-1}) \tag{6}$$

and then (5), (6) with (3) are equivalent to

$$\operatorname{Norm}_{\mathbf{Q}(\zeta)/\mathbf{Q}}\left(\prod_{i=2}^{p-1} \frac{\alpha-\alpha_i}{\zeta-\zeta^i}\right) = 1. \tag{7}$$

Up to equivalence, put

$$\alpha = b_1\zeta + b_2\zeta^2 + \cdots b_{p-2}\zeta^{p-2}, \qquad b_j \in \mathbf{Z}, \tag{8}$$

so that for $i = 2, \ldots, p-1$

$$q_i(\zeta) = \frac{\alpha - \alpha_i}{\zeta - \zeta^i} = b_1 + b_2\left(\frac{\zeta^2 - \zeta^{2i}}{\zeta - \zeta^i}\right) + \cdots + b_{p-2}\left(\frac{\zeta^{p-2} - \zeta^{(p-2)i}}{\zeta - \zeta^i}\right). \tag{9}$$

By (7), it is certainly necessary and sufficient for α to have index 1, that each $q_i(\zeta)$, $i = 2, \ldots, p-1$, at (9), be a unit in $\mathbf{Z}[\zeta]$. Notice

$$q_i(\zeta) = q_{i^*}(\zeta^i), \qquad ii^* \equiv 1 \bmod p \tag{10}$$

so that in fact the $(p-2)$ cyclotomic integers $q_i(\zeta)$ fall into $(p-3)/2$ pairs of conjugate integers, with $q_{p-1}(\zeta)$ invariant under the automorphism $\zeta \to \zeta^{-1}$, and hence lying in the maximal real subfield of $\mathbf{Q}(\zeta)$. In particular, it is necessary and sufficient that certain $(p-3)/2 + 1$ of the $q_i(\zeta)$ are units of $\mathbf{Z}[\zeta]$.

THEOREM. *Let* $\alpha = \zeta + \zeta^2 + \cdots + \zeta^{(p-1)/2} \in \mathbf{Z}[\zeta]$. *Then* α *has index* 1 *in* $\mathbf{Z}[\zeta]$.

Proof. The $q_i(\zeta)$ defined at (9) is as follows:

$$q_i(\zeta) = 1 + \frac{\zeta^2 - \zeta^{2i}}{\zeta - \zeta^i} + \cdots + \frac{\zeta^{(p-1)/2} - \zeta^{((p-1)/2)i}}{\zeta - \zeta^i}. \tag{11}$$

The fact that $q_i(\zeta)$ is a unit in $\mathbf{Z}[\zeta]$ will follow from the identity (12), using the well-known fact that $\zeta^r + \zeta^{-r}$, $r \in \mathbf{Z}$, is a unit of $\mathbf{Z}[\zeta]$.

LEMMA.

$$\zeta^{(1+i)/2}(\zeta^{1/4} + \zeta^{-1/4})(\zeta^{i/4} + \zeta^{-i/4})(\zeta^{(i-1)/4} + \zeta^{-(i-1)/4})\, q_i(\zeta) = -1 \tag{12}$$

(*where the exponents of* ζ *are treated as integers modulo* p).

Proof. Let

$$\sigma_r = \zeta^r + \zeta^{-r}; \qquad \tau_r = \zeta^r - \zeta^{-r}$$

so that

$$(\zeta-\zeta^i)\,q_i(\zeta)=(\zeta-\zeta^i)+(\zeta^2-\zeta^{2i})+\cdots+(\zeta^{(p-1)/2}-\zeta^{((p-1)/2)i})$$
$$=\frac{1}{2}\sum_{k=1}^{(p-1)/2}(\sigma_k-\sigma_{ki}+\tau_k-\tau_{ki})$$
$$=\frac{1}{2}\sum_{k=1}^{(p-1)/2}(\tau_k-\tau_{ki})$$

since $\sum_{k=1}^{(p-1)/2}\sigma_k=\sum_{k=1}^{(p-1)/2}\sigma_{ki}=0$.

To verify (12), it is therefore sufficient to verify

$$\frac{1}{2}\zeta^{(1+i)/2}\sigma_{1/4}\sigma_{i/4}\sigma_{(i-1)/4}\sum_{k=1}^{(p-1)/2}(\tau_k-\tau_{ki})$$
$$=-(\zeta-\zeta^i)=\zeta^{(1+i)/2}\tau_{(i-1)/2},$$

i.e.,

$$\frac{1}{2}\sigma_{1/4}\sigma_{i/4}\sigma_{(i-1)/4}\sum_{k=1}^{(p-1)/2}(\tau_k-\tau_{ki})=\tau_{(i-1)/2}. \tag{13}$$

Now σ_r, τ_s satisfy the relations

$$\sigma_r\sigma_s=\sigma_{r+s}+\sigma_{r-s};\qquad \sigma_r\tau_s=\tau_{r+s}-\tau_{r-s};\qquad \tau_r\tau_s=\sigma_{r+s}-\sigma_{r-s} \tag{14}$$

and in particular,

$$\sigma_r\tau_r=\tau_{2r}. \tag{15}$$

Using (14), (15), then (13) is equivalent to

$$\frac{1}{2}(\sigma_{(1+i)/4}+\sigma_{(1-i)/4})\sum_{k=1}^{(p-1)/2}(\tau_k-\tau_{ki})=\tau_{(i-1)/4} \tag{16}$$

and using the second relation at (14), (16) is equivalent to

$$\frac{1}{2}\sum_{k=1}^{(p-1)/2}\{(\tau_{(1+i)/4+k}+\tau_{(1-i)/4+k}+\tau_{(1+i)/4-ik}+\tau_{(1-i)/4-ik})$$
$$-(\tau_{(1+i)/4-k}+\tau_{(1-i)/4-k}+\tau_{(1+i)/4+ik}+\tau_{(1-i)/4+ik})\}=\tau_{(i-1)/4}. \tag{17}$$

Now for $1\leqslant k,\ k'\leqslant(p-1)/2$, then $((1+i)/4+k)+((1-i)/4+k')\equiv 0 \bmod p$ precisely when $k+k'=(p-1)/2$. Moreover, $\tau_a+\tau_b=0$ when $a+b\equiv 0 \bmod p$. Thus

$$\sum_{k=1}^{(p-1)/2}(\tau_{(1+i)/4+k}+\tau_{(1-i)/4+k})=\tau_{(i-1)/4}+\tau_{-(i+1)/4}.$$

Similarly

$$\sum_{k=1}^{(p-1)/2} (\tau_{(1+i)/4-ik} - \tau_{(1-i)/4+ik}) = 0,$$

$$\sum_{k=1}^{(p-1)/2} (\tau_{(1-i)/4-ik} - \tau_{(1+i)/4+ik}) = \tau_{(i+1)/4} - \tau_{(1-i)/4},$$

and

$$\sum_{k=1}^{(p-1)/2} (\tau_{(1+i)/4-k} + \tau_{(1-i)/4-k}) = 0.$$

Thus, the sum on the left hand side of (17) is equal to

$$\tfrac{1}{2}(\tau_{(i-1)/4} + \tau_{(i+1)/4} + \tau_{(i+1)/4} - \tau_{(1-i)/4})$$

which equals $\tau_{(i-1)/4}$ as required.

3

With $\alpha(\zeta) = \zeta + \cdots + \zeta^{(p-1)/2}$ then $\alpha(\zeta) + \alpha(\zeta^{-1}) = -1$ and so up to equivalence the conjugates of $\alpha(\zeta)$ represent just $(p-1)/2$ distinct elements. For a given prime $p \geqslant 5$, it is thus evident that there are up to equivalence at least $\frac{3}{2}(p-1)$ integers of index 1, corresponding to ζ, $\alpha(\zeta)$, and the conjugates of these elements. For $p = 3$, then $\zeta = \alpha(\zeta)$, and moreover ζ, ζ^2 are equivalent; so there is precisely one integer, ζ, in $S(\zeta)$. For $p = 5$, Nagell [5] demonstrates that the six integers characterized above are the only elements of $S(\zeta)$.

We show here that for $p = 7$, then again $S(\zeta)$ comprises precisely the nine integers characterized above.

THEOREM. *Let* $\zeta^7 = 1$. *If* $\alpha \in \mathbf{Z}[\zeta]$ *has index* 1, *then up to equivalence* $\alpha = \zeta, \zeta + \zeta^2 + \zeta^3$, *or one of the conjugates of these elements.*

Proof. As in (8), put $\alpha = b_1\zeta + b_2\zeta^2 + \cdots + b_{p-2}\zeta^{p-2}$, $b_j \in \mathbf{Z}$, with $q_i(\zeta)$ as in (9). Then by previous remarks it is necessary and sufficient for α to have index 1, that $q_2(\zeta)$, $q_3(\zeta)$, and $q_6(\zeta)$ be units of $\mathbf{Z}[\zeta]$.

Now the units of $\mathbf{Z}[\zeta]$ are of type $\pm\zeta^m\eta_0^r\eta_1^s$, $m, r, s \in \mathbf{Z}$, with $\eta_0 = \zeta + \zeta^6$, $\eta_1 = \zeta^3 + \zeta^4$ (see, for example, Edwards [2, Section 6.9]). It follows that there exist m_i, r_i, $s_i \in \mathbf{Z}$ such that

$$\zeta^{m_i} q_i(\zeta) = \pm\eta_0^{r_i}\eta_1^{s_i}.$$

Since η_0, η_1 are real, then $\zeta^{m_i} q_i(\zeta)$ is real for some $m_i \in \mathbf{Z}$. Then

$$\zeta^{m_i} q_i(\zeta) = \zeta^{-m_i} q_i(\zeta^{-1}). \tag{18}$$

Writing out the $q_i(\zeta)$:

$$\begin{aligned} q_2(\zeta) &= (b_1 - b_4) + \zeta(b_2 - b_4) \\ &\quad + \zeta^2(b_2 + b_3 - b_4 - b_5) + \zeta^3(b_3 - b_5) + \zeta^4 b_3 \\ q_3(\zeta) &= (b_1 - b_3 + b_4 - b_5) + \zeta(b_2 - b_3) \\ &\quad + \zeta^2(b_4 - b_5) + \zeta^3(b_2 - b_3 + b_4) + \zeta^5(-b_3 + b_4) \\ q_6(\zeta) &= (b_1 + b_3 - b_4) + (\zeta + \zeta^6)(b_2 - b_5) + (\zeta^2 + \zeta^5)(b_3 - b_4). \end{aligned}$$

Consider $i = 2$.

From $m_2 = 0$, (18) implies $b_2 = b_4$; $b_3 = b_5 = 0$;
From $m_2 = 1$, (18) implies $b_1 = b_2 = b_4$; $b_3 = 0$;
From $m_2 = 2$, (18) implies $b_1 = b_4$; $b_3 = b_5 = 0$;
From $m_2 = 3$, (18) implies $b_1 = b_2 = b_4$; $b_3 = b_5$;
From $m_2 = 4$, (18) implies $b_1 = b_2 = b_4$; $b_5 = 0$;
From $m_2 = 5$, (18) implies $b_1 = b_2 + b_5 = b_3 + b_4$;
From $m_2 = 6$, (18) implies $b_1 = b_2$; $b_3 = b_5 = 0$.

Consider $i = 3$.

From $m_3 = 0$, (18) implies $b_2 = b_3 = b_5$; $b_4 = 0$;
From $m_3 = 1$, (18) implies $b_1 = b_5 = 0$; $b_2 = b_3$;
From $m_3 = 2$, (18) implies $b_1 = b_2 + b_5 = b_3 + b_4$;
From $m_3 = 3$, (18) implies $b_1 = b_2 = 0$; $b_4 = b_5$;
From $m_3 = 4$, (18) implies $b_1 = b_3$; $b_2 = b_4 = b_5$;
From $m_3 = 5$, (18) implies $b_1 = b_5$; $b_3 = b_4 = 0$;
From $m_3 = 6$, (18) implies $b_1 = b_3 = b_4$; $b_2 = 0$.

The only possibilities for m_2, m_3 which result in a non-zero α are the following: $(m_2, m_3, \alpha) = (0, 0, \zeta)$, $(1, 6, \zeta^5)$, $(2, 5, \zeta^2)$, $(3, 4, \zeta^6)$, $(4, 3, \zeta^3)$, $(6, 1, \zeta^4)$, and $(m_2, m_3) = (5, 2)$ with $b_1 = b_2 + b_5 = b_3 + b_4$. It remains only to investigate further this latter case $(m_2, m_3) = (5, 2)$.

Now

$$\begin{aligned} \zeta^5 q_2(\zeta) &= (-b_3 + b_5)(\zeta + \zeta^6) + (-b_3 + 2b_5)(\zeta^2 + \zeta^5) \\ &\quad + (-2b_3 + 2b_5)(\zeta^3 + \zeta^4) \end{aligned}$$

$$\zeta^2 q_3(\zeta) = (b_3 - b_4)(\zeta + \zeta^6) + (b_3 + b_4 - b_5)(\zeta^2 + \zeta^5) + (b_3 - b_5)(\zeta^3 + \zeta^4)$$

$$q_6(\zeta) = (-b_3 + b_4 - 2b_5)(\zeta + \zeta^6) + (-b_3 - b_4)(\zeta^2 + \zeta^5) - 2b_3(\zeta^3 + \zeta^4)$$

and since

$$\text{Norm}_{\mathbf{Q}(\zeta)/\mathbf{Q}}[a(\zeta + \zeta^6) + b(\zeta^2 + \zeta^5) + c(\zeta^3 + \zeta^4)] = (a + b + c)^3 - 7(ab^2 + bc^2 + ca^2 + abc)$$

then

$$\text{Norm}\, \zeta^5 q_2(\zeta) = -b_3^3 - 5b_3^2 b_5 + 8b_3 b_5^2 - b_5^3 \tag{19}$$

$$\text{Norm}\, \zeta^2 q_3(\zeta) = -b_3^3 + 2b_3^2 b_5 + b_3 b_5^2 - b_5^3 + 7b_4(-b_3 b_5 + b_5^2) + 7b_4^2(b_3 - 2b_5) + 7b_4^3 \tag{20}$$

$$\text{Norm}\, q_6(\zeta) = -b_3^3 + 2b_3^2 b_5 + 8b_3 b_5^2 - 8b_5^3 + 7b_4 b_5^2 + 7b_4^2(-b_3 + 2b_5) - 7b_4^3. \tag{21}$$

Modulo 7, these three expressions are congruent, so the condition that the $\zeta^{m_i} q_i(\zeta)$ be units may, without loss of generality, be expressed by equating the above three expressions to -1.

Subtracting (19) from (20) and (21), respectively, gives

$$b_3^2 b_5 + b_3(b_4^2 - b_4 b_5 - b_5^2) + (b_4^3 - 2b_4^2 b_5 + b_4 b_5^2) = 0$$

$$b_3^2(b_4 + b_5) + b_3(-b_4^2) + (-b_4^3 + 2b_4^2 b_5 - b_5^3) = 0.$$

Eliminating b_3,

$$b_4(b_4 - b_5)(b_4^3 + b_4^2 b_5 - 2b_4 b_5^2 - b_5^3)^2 = 0.$$

Since the cubic factor is irreducible (indeed, a norm from the maximal real subfield of $\mathbf{Q}(\zeta)$) the only possibilities are $b_4 = 0$ or $b_4 = b_5$. This in turn leads to

(i) $b_4 = 0,\ b_5 = 0,\ b_3 = 1;\ b_1 = 1,\ b_2 = 1;$

(ii) $b_4 = 0,\ b_3 = b_5 = -1;\ b_1 = -1,\ b_2 = 0;$

(iii) $b_4 = b_5 = -1,\ b_3 = 0;\ b_1 = -1,\ b_2 = 0;$

with $\alpha = \zeta + \zeta^2 + \zeta^3,\ -\zeta - \zeta^3 - \zeta^5,\ -\zeta - \zeta^4 - \zeta^5$, as required.

4

More generally, if $q_i(\zeta)$ defined in (9) is to be a unit in $\mathbf{Z}[\zeta]$, then (see, for example, Washington [6, Proposition 1.5]) there exists $m_i \in \mathbf{Z}$ such that $\zeta^{m_i} q_i(\zeta)$ is a unit of $\mathbf{Z}[\zeta + \zeta^{-1}]$; in particular, such that $\zeta^{m_i} q_i(\zeta)$ is real. It seems plausible that the only possibilities for the integers $\{m_i\}$ such that there do exist $b_i \in \mathbf{Z}$ with $\zeta^{m_i} q_i(\zeta)$ real, for $i = 2, \ldots, p-1$ (and $q_i(\zeta) \neq 0$), are given by $m_i = \lambda((i+1)/2)$ for a fixed $\lambda \in \mathbf{Z}$, $0 \leqslant \lambda \leqslant p-1$. This is trivially the case for $p = 3, 5$, is shown to be the case for $p = 7$ in the preceding section, and has been verified by hand for $p = 11$. Certainly with these values of $\{m_i\}$, the $\{b_i\}$ may be shown to exist as follows.

LEMMA. *Suppose* $\zeta^{\lambda((1+i)/2)} q_i(\zeta)$ *is real and non-zero,* $i = 2, \ldots, p-1$. *If*

(i) $\lambda = 1$, *then* $b_1 = b_2 + b_{p-2} = \cdots = b_{(p-1)/2} + b_{(p+1)/2}$;

(ii) $\lambda = 2$, *then* $b_1 = b_2 = \cdots = b_{p-2}$;

(iii) $\lambda \neq 1, 2$, *then* $b_k = 0$, $k \neq 1 - \lambda$ (*suffix taken modulo* p).

Proof.

$$
\begin{aligned}
q_i(\zeta) &= \sum_{r=1}^{p-2} b_r \left(\frac{\zeta^r - \zeta^{ri}}{\zeta - \zeta^i} \right) \\
&= \sum_{r=1}^{p-2} b_r \zeta^{(r-1)((1+i)/2)} \left(\frac{\zeta^{r((1-i)/2)} - \zeta^{-r((1-i)/2)}}{\zeta^{(1-i)/2} - \zeta^{-((1-i)/2)}} \right) \\
&= \sum_{r=1}^{p-2} b_r \zeta^{(r-1)((1+i)/2)} \frac{\tau_{r((1-i)/2)}}{\tau_{(1-i)/2}} \qquad (22)
\end{aligned}
$$

using former notation.

Put $k_i = (\lambda - 1)((1+i)/2)$. Then, since $\zeta^{\lambda((1+i)/2)} q_i(\zeta) = \zeta^{k_i + (1+i)/2} q_i(\zeta)$ is real, it follows that

$$
\zeta^{k_i + (1+i)/2} q_i(\zeta) = \zeta^{-k_i - (1+i)/2} q_i(\zeta^{-1}) \qquad (23)
$$

and thus from (22) (using $\tau_{-m} = -\tau_m$),

$$
\begin{aligned}
&\sum_{r=1}^{p-2} b_r \zeta^{r((1+i)/2) + k_i} \frac{\tau_{r((1-i)/2)}}{\tau_{(1-i)/2}} \\
&\qquad = \sum_{r=1}^{p-2} b_r \zeta^{-r((1+i)/2) - k_i} \frac{\tau_{r((1-i)/2)}}{\tau_{(1-i)/2}}. \qquad (24)
\end{aligned}
$$

Multiplying throughout by $\tau_{(1-i)/2}$:

$$
\sum_{r=1}^{p-2} b_r \tau_{r((1-i)/2)} \tau_{r((1+i)/2) + k_i} = 0
$$

and then using the third relation in (14),

$$\sum_{r=1}^{p-2} b_r(\sigma_{r+k_i} - \sigma_{ri+k_i}) = 0. \tag{25}$$

Introduce the integers $b_0 = b_{p-1} = 0$; so that (25) is equivalent to

$$\sum_{r=0}^{p-1} b_r(\sigma_{r+k_i} - \sigma_{ri+k_i}) = 0. \tag{26}$$

Denoting by i^* the inverse of i modulo p, then (26) can be rewritten

$$\sum_{r=0}^{p-1} \sigma_r(b_{r\ \ k_i} - b_{i^*(r-k_i)}) = 0, \tag{27}$$

where the suffices of the b_i are taken to be the least positive residues modulo p. Then (27) in turn can be written

$$2(b_{-k_i} - b_{-i^*k_i}) + \sum_{r=1}^{(p-1)/2} \sigma_r(b_{r-k_i} + b_{-r-k_i} - b_{i^*(r-k_i)} - b_{i^*(-r-k_i)}) = 0. \tag{28}$$

From the known dependence relation between the σ_r, it follows that

$$\begin{aligned} 2(b_{-k_i} - b_{-i^*k_i}) = b_{r-k_i} + b_{-r-k_i} - b_{i^*(r-k_i)} \\ - b_{i^*(-r-k_i)}, \qquad r = 1, 2, \ldots, \frac{p-1}{2}. \end{aligned} \tag{29}$$

Adding the $(p-1)/2$ equations at (29),

$$\begin{aligned} (p-1)[b_{-k_i} - b_{-i^*k_i}] &= \sum_{r=1}^{p-1} b_{r-k_i} - \sum_{r=1}^{p-1} b_{i^*(r-k_i)} \\ &= -(b_{-k_i} - b_{-i^*k_i}), \end{aligned}$$

so that

$$b_{-k_i} = b_{-i^*k_i}; \tag{30}$$

and from (29),

$$b_{r-k_i} + b_{-r-k_i} = b_{i^*(r-k_i)} + b_{i^*(-r-k_i)}, \qquad r = 1, 2, \ldots, \frac{p-1}{2}. \tag{31}$$

Consider the case $\lambda = 1$. Then $k_i = 0$, for each $i = 2, ..., p-1$. The equations (31) become

$$b_r + b_{-r} = b_{i^* r} + b_{-i^* r}, \qquad r = 1, 2, ..., \frac{p-1}{2}, \tag{32}$$

and so $b_1 + b_{-1} = b_{i^*} + b_{-i^*} = b_{i^{*2}} + b_{-i^{*2}} = \cdots$, and taking i to be a primitive root modulo p,

$$b_1 = b_2 + b_{p-2} = \cdots = b_{(p-1)/2} + b_{(p+1)/2}. \tag{33}$$

This verifies part (i) of the lemma.

Consider second the case $\lambda \neq 1$. Then $k_i = \mu((1+i)/2)$, $\mu = \lambda - 1$, $i = 2, ..., p-1$. From (30)

$$b_{-\mu((1+i)/2)} = b_{-\mu((1+i^*)/2)} \tag{34}$$

and taking $r = \mu((1+i)/2)$ in (31),

$$b_{-\mu(1+i)} = b_{-\mu(1+i^*)}. \tag{35}$$

Put $i = -((r+2)/r)$ $(r \neq 0, -2)$ in (34) to give

$$b_{\mu r^*} = b_{-\mu(r+2)^*}; \tag{36}$$

Put $i = -((r+1)/(r+2))$ $(r \neq -1, -2)$ in (35) to give

$$b_{-\mu(r+2)^*} = b_{\mu(r+1)^*}. \tag{37}$$

Then (36), (37) imply

$$b_{\mu r^*} = b_{\mu(r+1)^*} \qquad (r \neq 0, -1, -2)$$

whence

$$b_\mu = b_{\mu 2^*} = b_{\mu 3^*} = \cdots = b_{\mu(p-2)^*},$$

i.e.,

$$b_\mu = b_{2\mu} = b_{3u} = \cdots = b_{(p-2)\mu}. \tag{38}$$

Now $\lambda = 2$ gives $\mu = 1$ and $b_1 = b_2 = \cdots = b_{p-2}$. If $\lambda \neq 1, 2$ then $\mu \neq 0, 1$ and one of the terms at (38) is b_{p-1}, which is zero; thus, $b_j = 0$ for $j \neq 1 - \lambda$. This verifies parts (ii), (iii) of the lemma.

We can formulate a much stronger conjecture than on the integers $\{m_i\}$ above.

CONJECTURE. *If $\alpha \in \mathbf{Z}[\zeta]$ is of index 1, then up to equivalence $\alpha = \zeta$, $\zeta + \zeta^2 + \cdots + \zeta^{(p-1)/2}$, or one of the conjugates of these elements.*

REFERENCES

1. A. BREMNER, Integral generators in a certain quartic field and related Diophantine equations, *Michigan Math. J.* **32** (1985), 295–319.
2. H. M. EDWARDS, "Fermat's Last Theorem," Springer-Verlag, New York, 1977.
3. J. H. EVERTSE, On the representation of integers by binary cubic forms of positive discriminant, *Invent. Math.* **73** (1983), 117–138; corrigendum, *Invent. Math.* **75** (1984), 379.
4. K. GYÖRY, Sur les polynômes à coefficients entier et de discriminant donné, III, *Publ. Math. Debrecen* **23** (1976), 141–165.
5. T. NAGELL, Sur les discriminants des nombres algébriques, *Ark. Mat.* **7**, 19 (1967), 265–282.
6. L. C. WASHINGTON, "Introduction to Cyclotomic Fields," Springer-Verlag, New York, 1982.